REMARKS:

In the outstanding Office Action, claims 1-16 were rejected. Claims 1, 8, 15 and 16 are amended and new claim 17 has been added. No new matter has been added. Thus, claims 1-17 are pending and under consideration. The outstanding rejections are traversed below.

REJECTION UNDER 35 U.S.C. § 103(a):

Claims 1-16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over two or more of the following: Design of Conventional Cryptographic Algorithms reference by Preneel et al. (Preneel), U.S. Patent No. 6,501,840 (Saijo) and U.S. Patent No. 6,182,216 (Luyster).

Preneel is directed to extending output bits of S-boxes based on fast cache memory, and discusses the need to fit the S-boxes in the fast cache memory. In Preneel, S-boxes where 8 input bits are transformed into 32 or 64 output bits are discussed, and it is indicated that value of S-boxes is selected at random or to achieve certain properties of an encryption standard (i.e., DES) (see, page 113, paragraph 3 in section 4.2). That is, the Preneel design approach is limited to selecting a value for the S-boxes at random or in accordance with encryption standard used, and does not teach or suggest adaptively selecting the input bits of S-boxes in accordance with capacity of a memory.

The Examiner relies on Saijo as disclosing the selection of an input and output bit number of the S-boxes and generating each of the S-boxes with the input and output number selected. However, Saijo is directed to preventing a need to change design of an apparatus when a new cryptographic processing type or a new algorithm type is devised (see, col. 2, lines 55-64), and thus, the input/output bits are predetermined based on the input data size (see, column 5, lines 51-55). This means that Saijo is limited to calculating the input and the output bits based on a preset size of the data being transferred from a cryptographic processing unit.

Luyster encrypts a predetermined 128-bit or more input block and divides the input block into data segments using minimum size of round segments (see, col. 16, lines 59-64). However, the block size in Luyster is not variable and the minimum size of the round segments rotated by a data dependent variable is limited to at least 32 bits (see, col. 16, lines 63-65).

In contrast, the present invention determines both the input and output bit of S-boxes in accordance with parameters related to a capacity of a memory of a cipher device, an entire input/output bit of the block and the smallest input/output bit numbers of the S-boxes. This reduces the number of times the S-boxes is required to be accessed.

Independent claims 1, 8, 15 and 16 as amended recite that the input and output bit number of the S-boxes is selected based on "a memory capacity of a high-speed referable memory provided to said cipher device, a minimum input and output number of the S-boxes and an entire input and output numbers of the block".

Further, the present invention selects an input and output bit number of the S-boxes "based on a memory capacity of a high-speed referable memory provided to said cipher device, a minimum input and output number of the S-boxes and an entire input and output numbers of the block". For example, for a 32-bit nonlinear transformation where the processor includes a memory having 32 Kbytes, the 32 input bits are divided into 11, 10, 11 where only three S-boxes are used (see, FIG. 2 and corresponding text of the present application). Accordingly, processing speed is increased by as much as 25% according to the cipher logic design method of the present invention in comparison to Preneel.

It is respectfully submitted that independent claims 1, 8, 15 and 16 are distinguishable over the cited references.

For at least the above-mentioned reason, dependent claims depending from independent claims 1, 8 and 15 are patentably distinguishable over the combination of the cited references. For example, as recited in claim 3, "said selecting unit selects the input and output bit number of each S-box in such a manner that a sum of sizes of said plurality of S-boxes becomes largest within a memory capacity of a primary cache memory installed in a processor provided to said cipher device". The cited references, either alone or in combination, do not teach or suggest, a selecting unit that "selects the input and output bit number of each S-box in such a manner that a sum of sizes of said plurality of S-boxes becomes largest within a memory capacity of a primary cache memory installed in a processor provided to said cipher device", as recited in dependent claim 3.

Therefore, withdrawal of the outstanding rejection is respectfully requested.

NEW CLAIM:

New claim 17 is added herein to recite that the present invention includes, "determining an optimal input and output number of the S-boxes by generating a combination table having various sets of input and output numbers of the S-boxes enclosable in a memory of the cipher device" and "implementing the F-function by selecting one of the sets of input and output numbers of the S-boxes in the combination table".

Applicants respectfully submit that new claim 17 is patentably distinguishable over the cited references because the cited references do not teach or suggest, determining an optimal input and output number of the S-boxes based on "a combination table having various sets of input and output numbers of the S-boxes enclosable in a memory of the cipher device" and "implementing the F-function by selecting one of the sets of input and output numbers of the S-boxes in the combination table", as recited in new claim 17.

CONCLUSION:

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 6/2/5

By: _____

J. Randall Beckers
Registration No. 30,358

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501